УДК 004.056.53

АНАЛІЗ КОНЦПЕПЦІЇ BYOD ТА АРХІТЕКТУРА ДЛЯ ЇЇ ВПРОВАДЖЕННЯ

М. В. Кучменко[1], М. В. Грайворонський[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

У даній роботі розглядається концепція BYOD та необхідність її запровадження. Також визначені загрози, розглянуті різні підходи до реалізації концепції та їх недоліки. Розроблена архітектура BYOD, яка гарантує безпеку корпоративних даних у сукупності зі стратегією та політикою компанії.

Ключові слова: концепція BYOD, безпека корпоративної інформації, загрози, підходи до реалізації, архітектура, політика.

Вступ

З бурхливим розвитком технологій мобільних комунікацій, багато підприємств стикається з проблемою, як дозволити своїм співробітникам використовувати їх власні мобільні пристрої у виробничій діяльності і при цьому гарантувати безпеку корпоративних даних.

Концепція Bring Your Own Device (BYOD) (в перекладі – Принеси Свій Власний Пристрій) фокусується на вирішенні саме цього завдання. Застосування концепції BYOD на підприємстві дозволяє, крім корпоративних комп'ютерів, використовувати ще і особисті мобільні пристрої співробітників. Таке використання особистих пристроїв з будь-якої точки світу, забезпечує підвищення продуктивності праці і задоволеність працівників умовами роботи [1].

Прискорені темпи поширення BYOD змушують шукати баланс між мобільністю співробітників і інформаційною безпекою бізнесу, вирішуючи нові завдання, пов'язані з управлінням персональними пристроями, забезпеченням корпоративної безпеки і захистом персональних даних працівників.

1. Необхідність запровадження концепції BYOD і пов'язані з цим ризики

На сьогоднішній день відбувається прискорений розвиток комп'ютерної техніки. Якщо у конкретного користувача є можливість раз або два на рік купувати смартфон або планшет, більшість компаній не може собі дозволити дуже часто оновлювати робочу техніку для усіх своїх співробітників.

Така ситуація часто призводить до того, що співробітники починають користуватись своїми власними пристроями в робочих цілях. А це, в свою чергу, означає можливість розповсюдження корпоративної інформації, яка в результаті стає абсолютно незахищеною [2].

Саме тому постає необхідність запровадження концепції BYOD, яка гарантуватиме безпеку корпоративних даних на персональних пристроях співробітників і стане своєрідним компромісом між особистим і корпоративним.

Головна ціль концепції BYOD постає в тому, щоб персональні мобільні пристрої співробітників використовувались безпечно. Безумовною перевагою BYOD, окрім можливості самостійного вибору пристрою користувачем, є доступ до роботи в будь-який час і в будь-якому місці і більша мобільність. Проте це суперечить стандартним вимогам IT до безпеки даних і підтримки та змушує підрозділ IT шукати інший підхід до цієї проблеми.

З BYOD-пристроями пов'язаний весь набір ризиків інформаційної безпеки: порушення цілісності, конфіденційності і доступності даних. [3]. Більш предметно можна зробити акцент на наступних ризиках:

- отримання доступу до корпоративних даних на пристрої у випадку його втрати або крадіжки;
- підключення до ресурсів компанії з використанням самого пристрою або даних з нього;
- використання пристрою для інших атак;
- перехоплення даних в мережі;
- заражені ноутбуки або планшети в офісі можуть завдати шкоди пристроям інших співробітників фірми через робочу мережу;
- випадково встановлені шкідливі застосунки або неліцензійне ПЗ може порушувати роботу інфраструктури IT і законодавство.

Компанії неминуче стикаються з питанням, що конкретно треба захищати і як це можна зробити. Можна виділити три різних рівні захисту в залежності від того, які пристрої використовуються в компанії.

1) Захист пристроїв (для корпоративних пристроїв) включає:

- впровадження технології управління пристроями (MDM);
- запровадження суворих політик безпеки для пристроїв;
- локальне шифрування даних на пристрої;
- створення захищених розділів (контейнерів) на пристроях.

2) Захист застосунків (для різнорідного середовища з великим парком рішень) має забезпечувати:
   - тісний зв'язок з розробниками застосунків на предмет безпеки;
   - безпечне поширення і оновлення програм;
   - орієнтованість на одну платформу або мультиплатформу;
   - побудова процесу безпечного розвитку інформаційних систем компанії.
3) Захист даних (для особистих мобільних пристроїв) складається з:
   - контролю зліпків пристроїв (*fingerprint*);
   - шифрування каналу передачі даних;
   - віртуалізації і віддаленого робочого стола;
   - забезпечення цілісності даних (контроль життєвого циклу даних).

2. Підходи до реалізації BYOD

На сьогоднішній день технології гарантування безпеки корпоративних мобільних пристроїв включають цілий ряд різнорідних рішень і підходів:

- керування налаштуваннями (MDM);
- комплексне управління відповідністю пристроїв (EMM);
- управління мобільними застосунками (MAM);
- захист даних (криптоконтейнери) і т. д.

Для концепції BYOD найбільш актуальним стає захист критичних корпоративних даних і того, як вони будуть зберігатися і використовуватися на пристроях співробітників. Основною ідеєю такого підходу є зручність і поділ доступу до особистих і корпоративних даних на одному пристрої.

Спочатку для таких цілей застосовувалися рішення MDM, які програмними засобами розмежовували доступ до інформації на мобільному пристрої. Він вимагав не тільки встановлення додаткового програмного забезпечення, але й налаштування прав доступу через засоби централізованого управління. На жаль, даний підхід потребував кардинальної зміни політик безпеки стосовно до особистих пристроїв і концепції BYOD, так як він фокусувався на захисті самого пристрою, а не даних [4].

В результаті на зміну класичним MDM-рішенням прийшли продукти з підтримкою захищених контейнерів (пісочниць), які жорстко розділили функціонал MDM і захист даних. З одного боку, засобами централізованого управління забезпечувався контроль відповідності пристрою вимогам політик безпеки, з іншого, окремий програмний компонент в рамках MDM-рішення створював зашифрований контейнер для роботи з даними. Недоліком такого підходу стало те, що такого роду рішення шифрування даних працюють далеко не з усіма застосунками.

Наступним логічним кроком у гарантуванні безпеки корпоративних даних стала технологія віртуалізації. Основною ідеєю віртуалізації стає концепція такого підходу, коли на одному пристрої співробітника створюються дві незалежні ОС або незалежні набори програмних компонентів (доменів) [5]. Один домен застосовується виключно в особистих цілях співробітника, другий – в робочих цілях. Більшість віртуальних рішень для мобільних пристроїв можна віднести до трьох основних груп за спрощеним варіантом реалізації:

1) Віртуальний робочий стіл (VDI і подібні рішення). Одна з найбільш усталених технологій із області віртуалізації, принцип роботи якої аналогічний стандартним рішенням для корпоративної інфраструктури з тонкими клієнтами. Користувач працює з віддаленим робочим столом, не маючи при цьому можливості зберегти будь що на своє локальне робоче місце.
2) Хмарна віртуалізація. В даному підході на кінцевому пристрої користувача присутні лише ярлики для доступу до застосунків, як зі своєї особистої ОС, так і з окремої оболонки, що створює подобу незалежного робочого стола або всієї операційної системи. При цьому всі дані зберігаються і обробляються на стороні хмарного хостингу, в якому відбувається розмежування доступу до застосунків і управління користувачами. До реалізації таких рішень існує два підходи:
   - послуга з хмарного хостингу самого розробника рішення, де компанії надається лише платформа для побудови політик і вибору з готового списку застосунків для співробітників;
   - продукт для приватної хмарної інфраструктури, що дозволяє створювати не тільки політики для поширених застосунків, але й додавати власні застосунки для доступу з пристроїв співробітників.
3) Віртуалізація на самому пристрої – це технологія прямого виконання віртуального середовища на кінцевому пристрої користувача. Дана модель передбачає пряме створення двох незалежних доменів на одному пристрої з можливістю швидкого перемикання між ними. Існують принципово різні варіанти реалізації такого функціоналу:
   - створення паралельно працюючих віртуальних доменів на єдиній апаратній платформі;
   - створення віртуального домену всередині реального операційного середовища мобільного пристрою.

Незаперечними плюсами підходів у вигляді віддалених робочих столів (VDI) і хмарної віртуалізації стає те, що застосунки виконуються, обробляють і зберігають критичні дані поза пристроями співробітників. З одного боку, це істотно знижує ризики, пов'язані з особистими пристроями, з іншого – пере-

дача і зберігання даних в разі стороннього хмарного хостингу схильна до додаткових ризиків.

Іншою великою проблемою є необхідність мати стабільний інтернет-канал для роботи з корпоративними даними і застосунками. Це може бути зручно у випадку використання співробітником пристрою на території компанії (Wi-Fi наприклад), але може виявитися абсолютно неприйнятним за її межами, коли співробітник відповідає за канал самостійно.

Проте, при всіх перевагах стратегії віртуалізації для компаній, вона може негативно відбитися на взаємодії з співробітниками. Перш за все, це пов'язано з питаннями продуктивності і енергоспоживання мобільних пристроїв. Паралельне створення двох віртуальних доменів і виконання віртуального середовища на існуючій ОС мобільного пристрою, безумовно, будуть вимагати ресурсів, що перевищують штатні запити пристрою. І якщо в результатом буде зниження продуктивності пристрою та прискорення розрядки акумулятора, користувач, як і раніше, буде працювати з пристроєм по-старому, без будь-яких засобів захисту.

3. Комплексна архітектура BYOD

Проаналізувавши кожен окремий підхід до реалізації концепції BYOD можна зробити висновок, що жоден із них повністю не гарантує безпеку корпоративної інформації на мобільних пристроях. Таке завдання потребує комплексного рішення. Тому враховуючи існуючі загрози для безпеки інформації та розглянувши різні підходи до побудови BYOD була розроблена архітектура рішення, яка, в комплексі зі стратегією та політикою безпеки окремої компанії, здатна забезпечити ефективність концепції BYOD та безпеку корпоративної інформації.

Найбільш ефективним рішенням гарантування безпеки даних на пристроях BYOD є надання доступу до інформаційних активів компанії через віддалене підключення BYOD-пристроїв через термінальні сесії до віртуальних середовищ. В свою чергу віртуальні середовища захищені за допомогою DLP-системи, яка функціонує у внутрішній мережі та забезпечує запобігання неконтрольованих витоків інформації.

Основними компонентами архітектури є (рис. 1):

- MDM – система використовується для контролю локальних застосунків на пристроях, віддаленого знищення даних, забезпечення надійного парольного захисту пристрою та шифрування даних. Ідентифікація та аутентифікація в MDM реалізується на основі цифрових сертифікатів і PKI. Як сховище сертифікатів і сервера аутентифікації використовуються корпоративні служби каталогів.
- Захищений контейнер, на якому розміщуються дані для безпечного зберігання за допомогою засобів шифрування. Захисту підлягають локальні кеші повідомлень електронної пошти, переглянуті веб-сторінки і дані з будь-яких мобільних застосунків. При необхідності повинна реалізовуватись аутентифікація, шифрування і вибіркове видалення даних, що підлягають захисту, не торкаючись персональних даних, які також знаходяться на BYOD-пристрої.

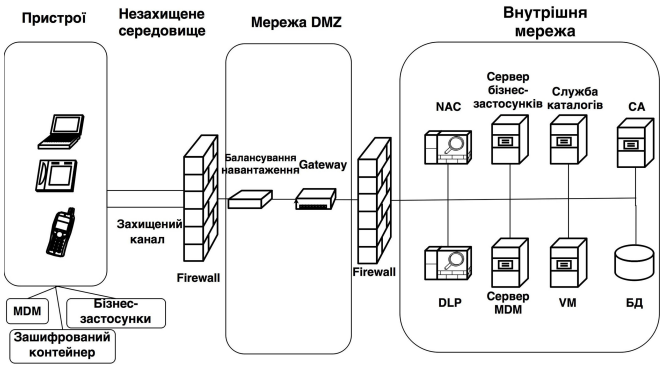

Рис. 1. Архітектура BYOD

- Захищений канал передачі даних реалізується шляхом створення VPN-підключень до корпоративної мережі або шляхом шифрування даних на рівні окремих застосунків (наприклад, шифрування електронної пошти або доступ до веб-сайтів по HTTPS).
- Network Access Control являє собою політику управління доступом до корпоративної пошти, застосунків, контенту і веб-трафіку. Політика повинна враховувати як дії користувача, так і налаштування на його BYOD-пристрої. В залежності від ступеню відповідності цих дій або налаштувань корпоративним стандартам, користувачеві надається той чи інший рівень доступу до ресурсів. BYOD-пристрої знаходяться під повним контролем користувачів, які можуть довільним чином безконтрольно змінювати налаштування політики безпеки на своїх пристроях. Тому постає завдання автоматичного визначення рівня довіри до підключеного BYOD-пристрою. Потім, в залежності від ступеня довіри, визначається рівень доступу до ресурсів корпоративної мережі.
- Бізнес-застосунки. Мобільні користувачі можуть використовувати у своїй діяльності досить широкий набір примітивних і незахищених мобільних застосунків, що завантажуються з незахищеного середовища. MDM має розмежовувати середовище захищених бізнес-застосунків, які обмінюються між собою корпоративними даними, і незахищене середовище застосунків користувача, які мають справу з персональними даними. Необхідно створити такі умови, у яких призначені для користувача програми не мали б доступу до захищеного середовища.
- Служба Каталогів гарантує доступ до даних віртуального робочого середовища тільки після авторизації облікового запису співробітника в домені служби каталогів. Доступ надається через захищений канал передачі даних, який, в свою чергу, використовує сувору аутентифікацію користувача та пристрою.
- VM – це віртуальна реалізація системи, що надає користувачам робоче середовище, в якому

можуть бути опубліковані і доступні необхідні для роботи програми та дані.

- DLP являє собою систему запобігання витоків даних, інтегровану у віртуальне робоче середовище. Вона забезпечує контроль доступних каналів передачі даних у конкретному віртуальному середовищі (електронна пошта, веб-сайти, месенджери, канал друку, переслані до віртуального середовища локальні USB-пристрої) для запобігання витоку даних з BYOD- пристрою. Компоненти DLP-системи здійснюють пошук і класифікацію інформації, що захищається за встановленими критеріями. SIEM формує «єдине вікно» для адміністратора безпеки, в якому зводяться дані про виявлені файли, які підлягають захисту, спроби доступу до них, а також пов'язується (корелюється) технологічна інформація, яка надходить від ОС, СУБД, мережевого обладнання та інших джерел, формуючи повну картину стану ІБ в організації.

Таким чином забезпечується виконання трьох ключових умов безпеки:

1) Безпечна обробка даних, коли співробітники не використовують власні застосунки для локальної обробки даних на пристрої BYOD при підключенні до корпоративного порталу на безпечній сесії, або можливість використання даних блокується на контекстному рівні. Таким чином гарантується, що корпоративні дані компанії не будуть поширені далі контрольованого пристрою.
2) Безпечне зберігання даних, коли захищені корпоративні дані можуть бути доступні тільки у віртуальному середовищі, а у разі редагування чи іншої зміни зберігаються тільки на сервері або можуть бути роздруковані на принтерах в корпоративній мережі. При цьому не допускається або контролюється локальне збереження даних у вбудованій пам'яті BYOD-пристроїв, на підключених знімних накопичувачах, друк на принтерах поза корпоративної мережі.
3) Моніторинг даних кожної сесії співробітника, який забезпечує фільтрацію змісту файлів і даних, що проходять через комунікаційні канали (електронна пошта, веб-сайти, месенджери і т.д.), канал друку, мережеві файлові ресурси, а також знімні носії, доступ до яких дозволений програмним забезпеченням віртуального хостингу.

4. Стратегія та політика в рамках концепції BYOD

Компанії повинні утримувати баланс поміж двома крайностями – повною свободою, якої прагнуть співробітники і тотальним контролем, якого прагне компанія. Гнучка і масштабована стратегія буде якнайкраще задовольняти зростаючий попит на BYOD. Політика BYOD має застосовуватись у комплексі та обов'язково включати в себе наступні компоненти:

1) Масштабованість пристроїв – означає, що платформи, ОС та пристрої постійно оновлюються. Тому гнучкі принципи повинні враховувати еволюціонування технологій і бажання співробітників користуватись найновішим обладнанням.
2) Критерії пристроїв – комплексні критерії оцінки, які повинні визначати, які пристрої допускаються до підключення до корпоративної системи, а які не відповідають усім вимогам і не задовольняють цим критеріям.
3) Сертифікація – означає, що усі застосунки повинні мати відповідні ліцензії та сертифікації та завантажуватись від надійних постачальників.
4) Критерії безпеки – заздалегідь визначають які корпоративні дані будуть вилучені і знищені у випадку втрати або крадіжки пристрою, а також кому належить право на використання корпоративних даних і застосунків. Окрім цього необхідно зробити певні обмеження до застосування деяких функцій пристрою, таких як відеокамера та зберігання відеозаписів. Також критерії безпеки повинні передбачати використання антивірусу та його регулярне оновлення.

У рамках програми BYOD повинна виконуватись чітка політика за типами пристроїв, яка б допомагала компаніям досягти певного рівня стандартизації та створенню необхідної інфраструктури для підтримки пристроїв. Обрана політика повинна враховувати специфіку виконуваної роботи, щоб визначити необхідні параметри персонального пристрою.

Висновки

На сьогоднішній день впровадження концепції BYOD стає необхідністю для більшості компаній. І це вимагає відповідних змін у роботі підрозділу IT з метою гарантування безпеки зберігання корпоративних даних. На сьогодні існують окремі підходи до захисту, які не є достатньо ефективними. Тому, враховуючи існуючі загрози для безпеки інформації, була розроблена архітектура BYOD, яка, в комплексі зі стратегією та політикою безпеки окремої компанії, здатна забезпечити ефективність концепції та безпеку корпоративної інформації.

Перелік використаних джерел

1. Hemmersbach R. What is hidden behind concepts BYOD, CYOD, COPE. — 2013.
2. Security controls. — 2017. — Access mode: `https://en.wikipedia.org/wiki/Security_controls`.
3. G. Thomson. Network Security BYOD. — 2012. — Access mode: `ScienceDirect.com`.
4. Bring your own device (BYOD) trends and audit considerations. — 2012. — Access mode: `http://www.sifma.org/uploadedfiles/bring`.
5. Johnson. K Barbara L. SANS Mobility/BYOD Security Survey. — 2012. — Access mode: `http://www.sans.org/reading_room.pdf`.